REMARKS

Reconsideration of the above-identified application in view of the amendments above and the remarks following is respectfully requested.

Claims 1-36 are currently pending.

The Examiner objected to the Abstract because it should be in one paragraph. In reply, Applicant has reformatted the abstract such that it appears as one paragraph.

The Examiner objected to Claims 2 and 31 because they contain informalities. These claims have, therefore, been amended so as to correct the informalities noted by the Examiner.

The Examiner rejected Claims 18-36, in accordance with 35 USC § 101.

Claims 1-8 and 17-31 are rejected under 35 USC § 102(b).

Claims 9-16 and 31-36 are rejected under 35 USC § 103(a).

Applicant has, therefore, amended Claims 18, 19, 21, 24, 26, and 31 so as to overcome the Examiner's rejection with regard to 35 USC § 101. It is submitted that no new subject matter has been added to these claims, and that support for these amendments may be found in the application, for example, at the following portions:

Claims 18 and 19: page 15, line 25
Claim 21: page 20, line 24
Claim 24: page 18, line 10
Claim 26: page 15, line 18
Claim 31: page 33, line 8

Claim Rejections – 35 USC § 102

In this section of the Office Action, Claims 1-8 and 17-31 were rejected under 35 USC § 103 (a) as being unpatentable over Caputo et al. (US Patent No. 5,546,463). Applicant respectfully traverses this rejection.

In response and in view of the amendments to Claims 18, 19, 21, 24, 26, and 31, it is submitted that there is no prima facie basis for the Examiner's assertion that these claims are anticipated by the teachings of Caputo et al, as will be discussed below.

Caputo et al. teach a security device which can be carried by a user and connected to telephone circuits. The device is used to authenticate the user to a network, computer system, or application program; and is used to encrypt data communications from the user (column 4, lines 24-29). The device itself does the authentication of the user, whereby authentication may include the user inputting a PIN number (column 6, lines 46-64). The device does not receive an authentication datagram by an intermediate device, nor does it protect the datagram by the intermediate device.

In contrast, Claim 1 recites "A method of authenticating, using an authentication server, the use of an authentication device over a communication network via an intermediate communication device, comprising: receiving an authentication datagram by said intermediate device; protecting said datagram by said intermediate device, by at least one of changing, adding to, encrypting and signing of said datagram; and forwarding said datagram to said authentication server for authentication."

Additionally in contrast to the teachings of Caputo et al., amended Claim 18 recites "A method of authentication of an authentication datagram by a remote authentication server, comprising: sending an encrypted datagram by secure computer communication from a vendor software to said remote authenticator; receiving said encrypted datagram by said remote authenticator; comparing said datagram or a hash thereof to a hash table at said server; generating a binary validation answer by said server without an associated explanation; and outputting said binary validation answer." Caputo et al. do not teach such a device wherein a validation answer is generated without an associated explanation.

Further in contrast to the teachings of Caputo et al., amended Claim 19 recites "A method of authentication of an authentication datagram by a remote authentication server, comprising: sending an encrypted datagram by computer communication from an authentication device to said remote authentication server; receiving said encrypted datagram by said remote authentication server; searching, at said server, for a hash value matching said datagram or a hash thereof; generating a validation answer by said remote authentication server, responsive to said search, wherein, said datagram includes a secret code and wherein said secret code exists only on said authentication device; and outputting said validation answer." Caputo et al. do not teach such a device including a secret code on an authentication device.

Further in contrast to the teachings of Caputo et al., amended Claim 21 recites "A method of generating a code set for a remote authentication device, comprising: providing a code generating software; providing at least one seed code for said software; generating said code set using said software and said seed; destroying said seed immediately after generating said code set; forwarding said code set to said remote authentication device; and storing said code set or an indication thereof on said remote authentication device." Caputo et al. do not teach such a device, wherein a seed code is destroyed after generating a code set.

Further in contrast to the teachings of Caputo et al., amended Claim 24 recites "A method of communication between a vendor and a user using an authentication device, comprising: generating a one time code for the user for a session; receiving an authentication datagram from said user; and forwarding said datagram to a remote authentication server for authentication if at least an indication of said one time code that matches said user is provided with said datagram." Caputo et al. do not teach a device having a one time code that matches the user with a datagram.

Further in contrast to the teachings of Caputo et al., amended Claim 26 recites "A method of remote validation, comprising: receiving an authentication datagram by an authentication server from a remote authentication device; matching said datagram or a hash of said datagram to a table; calculating a counter value from a matching position in said table; and if said authentication datagram is valid, increasing said counter over a previous counter, within a certain limit; and outputting a validation signal." Caputo et al. do not teach a device wherein a counter value is calculated.

Yet further in contrast to the teachings of Caputo et al., amended Claim 31 recites "A method of detecting a transmission of an acoustic multitone Frequency Shift Key (FSK) signal, comprising: receiving an acoustic signal; converting the signal into a Hilbert-transform representation of the signal; correlating said converted signal with at least one reference signal representing at least one expected frequency in said FSK signal; integrating said correlation over an interval; if a signal is present, based on a thresholding of a result of said integrating, generating a validation signal; and outputting said validation signal." Caputo et al. do not teach a device wherein a reference signal represents at least one expected frequency, nor do they teach integrating a correlated signal over an internal, nor do they teach generating a validation signal based on a thresholding of a result of the integrating.

In light of the above, it is submitted that independent Claim 1 and amended independent Claims 18, 19, 21, 24, 26, and 31 are not anticipated by Caputo et al. and are, therefore, allowable. It is further submitted that Claims 2-8, 17, 20, 22-23, 25, and 27-30 are allowable, as they depend from allowable claims.

Claim Rejections – 35 USC §103

In this section of the Office Action, Claims 9-16 and 31-36 were rejected under 35 USC § 103 (a) as being unpatentable over Caputo et al. in view of Daudelin (US Patent No. 4,716,376). Applicant respectfully traverses this rejection.

It is submitted that there is no prima facie basis for the Examiner's assertion that these claims are unpatentable, as will be discussed below.

Neither Caputo nor Daudelin teaches the limitation found in independent Claim 1, namely, "A method of authenticating, using an authentication server, the use of an authentication device over a communication network via an intermediate communication device," the method including "forwarding said datagram to said authentication server for authentication." Additionally, neither Caputo nor Daudelin teaches the limitation found in amended independent Claim 31, namely, "A method of detecting a transmission of an acoustic multitone Frequency Shift Key signal," the method including "converting the signal into a Hilbert-transform representation of the signal," "correlating said converted signal with at least one reference signal representing at least one expected frequency in said FSK signal," "integrating said correlation over an interval," and "outputting said validation signal."

It is submitted that, since these limitations found in the independent claims are not taught by the cited art, these claims are patentable.

As noted above, Caputo et al. teach a security device which itself does the authentication of the user. The device does not transmit signals to a remote location for authentication.

Daudelin teaches an FSK demodulator.

While the Examiner has stated that, since encryption coding is a well-known practice, "the skilled person would have been motivated to use such algorithm to communicate efficiently and securely in a distributed environment," the Examiner has produced no prior art reference that teaches authenticating, using an authentication server, the user of an authentication device over a communication network, via an intermediate communication device, as recited in Claim 1.

Applicant respectfully submits, therefore, that since it would not be obvious to employ an intermediate communication device for authentication, Claim 1 is patentable over Caputo et al. in view of Daudelin. It is further submitted that Claims 9-16 are allowable, as they depend from allowable Claim 1.

Additionally, while the Examiner has stated that it would have been obvious to one skilled in the art "to incorporate the teaching of Caputo with Daudelin's disclosure of transmitting signal [sic] from an 'authentication card,'" the Examiner has produced no prior art reference that teaches "detecting a transmission of an acoustic multitone Frequency Shift Key signal from a remote location," as recited in amended Claim 31.

In view of the foregoing discussion, it is submitted that independent Claim 31 is patentable over Caputo et al. in view of Daudelin. It is further submitted that Claims 32-36 are patentable, as they depend from allowable independent Claim 31.

All of the issues raised by the Examiner have been dealt with. In view of the foregoing, it is submitted that all the claims now pending in the application are allowable. An early Notice of Allowance is therefore respectfully requested.

Respectfully submitted,

Martin D. Moynihan

Martin D. Moynihan
Registration No. 40,338

Date: September 18, 2008

Enclosures:

- Petition for Extension (Three Months)